机房环境改造及系统建设参数要求

# 功能需求及技术参数

* 功能需求
* **动环系统：**实现UPS监控、配电监控、蓄电池监测、精密空调监测、漏水报警、温湿度监控、温湿度、消防报警监控、安防监控系统监控、门禁监控，所有工程含集成费。机房现有视频监控接入动环系统。

在机房入口设置门禁系统。门禁系统采用UPS供电，并与消防系统联动。当发生消防报警时，系统能够接收消防报警信号，并控制所有门为开门状态，配备适应现代管理需求的应用管理系统。支持密码+指纹识别，可远程设置密码及有效期限，可对门控器进行远程管理操作；实时监控每个门的状态，并对所有刷卡、开门、关门等事件进行记录。

* **接地系统：**根据我校机房环境完成机房接地系统的整体设计与施工。在机房内地板下及每排机柜前方安装铜排，机房内的所有金属物接入接地系统中。接地系统与室外大地连通。接地系统的室外预埋坑的开挖及恢复工作由学校协助完成。
* **消防系统：**机房设置火灾自动消防系统，实现自动检测火情、自动报警，并自动灭火。机房安装七氟丙烷气体自动灭火系统。投标人负责根据我校中心机房的物理环境完成相关的设计、施工工作，并协助完成验收工作。消防系统的设计、施工及所使用的设备和材料须符合国家消防气体灭火系统的相关法律规范和标准，并提供有关书面文件。消防系统接入机房动环系统。消防系统与门禁系统联动，发生火灾时自动打开门禁。根据学校消防监控实际需求，结合学校消防系统的实际情况，确定机房消防监控与学校中控室的连接方案。消防系统的设计、安装调试、集成等全部工作须在合同签署后的30个工作日内施工完毕。消防系统的承建单位负责承担本项目的售后及维保。承建单位须持有消防设施维护保养检测机构的资质。承建单位针对本消防系统及相关设备提供三年维保服务，包括：消防联动报警、气体灭火、消防泄压及排气、消防应急照明及疏散指示等系统维保及服务，消防演习、检查、培训等服务。施工要求：施工必须严格依照国家及地方相关施工规范进行施工。施工人员必须取得消防主管部门颁发的上岗证。施工人员必须严格依照安全文明施工管理规定进行施工。
* **防水工程：**精密空调四周制作防水围堰，防止空调冷凝水进入机房内对设备造成危害，确保积水不会扩散，且能正常排出。
* **机房其它改造内容：**机房照明改造，机房现有照明电源改接为UPS供电，增加机房照明亮度，保证光线明亮且柔和，照度均匀，无反光眩光，布局合理且操作方便。增配PDU，并完成相关线路施工。
* **日志审计系统：**部署一套日志集中管理平台，通过对日志进行集中采集和准实时索引，提供搜索、分析、可视化和监控告警等功能，实现线上业务实时监控、业务异常原因定位、业务日志数据统计分析、及安全与合规审计。
* **终端检测响应平台软件：**部署一套终端检测响应平台软件，实现终端安全可视，终端统一管理，统一策略下方，统一威胁处置，统一漏洞修复等功能。
* **防病毒网关：**在数据中心出口防火墙上部署防病毒功能模块。
* 技术参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 规格描述 | 单位 | 数量 |
|  | 现有机房改造建设 | 1、防雷接地，本次防雷接地必须达到相关标准，建设完成后接地电阻率不得超过4欧姆，能够提供相关设备进行检测，包括但不限于如下清单：  三相二级复合型电源防雷器≥1套；  智能防雷器≥1套；  99雷电计数器≥1套；  等电位连接箱≥3个；  接地铜排≥90米；  接地铜箔≥360米；  接地模块≥10个；  降阻剂≥10袋；  绝缘子≥105套；  接地扁钢≥36米；  防雷引线≥20米；  防雷引线≥120米；  辅材材料≥1项。  2、动环系统建设，包括但不限于如下清单：  智能电量仪≥1 个；  电流互感器≥3 个；  配电系统监测软件≥1套；  UPS系统监测软件 ≥1套；  精密空调系统监测软件≥1套；  不定位漏水检测≥1套；  漏水系统监测软件≥1套；  温湿度传感器≥4个；  温湿度监测软件≥1套；  烟感≥4个；  24V中间继电器≥1个；  消防系统监测软件≥1 套；  视频监控软件模块≥1套；  门禁控制器≥1套；  读卡器≥2个；  磁力锁-单开≥1个；  磁力锁-双开≥1个；  IC感应卡≥10张；  开门按钮≥2个；  门禁接入软件模块≥1套；  动环监控主机≥1台；  动力环境监控集中监控软件V1.0≥1套；  台式电脑≥1台；  声光报警器≥1个；  邮件报警软件≥1套；  短信语音报警软件≥1套；  SIM 手机卡≥1张；  APP安卓手机软件≥1套。  3、防水工程，精密空调四周制作防水围堰，拦水围堰宽12cm，高10cm，使用水泥及防水涂料等材料确保积水不会扩散，且能正常排出。  4、机房照明线路改造，照明采用UPS供电。安装LED格栅灯，改善机房照明，增配PDU。格栅灯≥12个；PDU≥5。  5、包含以上所有系统建设安装施工及辅材，项目实施过程中如遇到辅材的追加费用等均与采购人无关，由供应商自行承担。 | 项 | 1 |
| 2 | 日志审计系统 | 1、网口：≥6个千兆工作管理口（1管理口+1HA口+4审计口)，≥1个console口，内存：≥8GB，磁盘：≥4T\*1，日志处理能力EPS：≥4000/秒（峰值：5000/秒），双电源，资产授权数量：≥100个。  2、采用B/S架构，提供全中文Web管理界面，无需安装任意客户端软件或插件。产品获得公安部计算机信息系统安全产品销售许可证，并且审计结果存储于独立存储空间。  3、★支持多种日志收集方式，至少支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP等协议。自动识别各种日志类型，自动抽取关键字段，将非结构化日志转化为结构化数据；支持通过安装代理的方式提取并收集日志。支持采集网络设备（交换路由等）、安全设备、操作系统、应用系统、数据库、中间件、网管等资产的日志。自动解析主流网络设备、安全设备和中间件的日志数据。对日志、解析规则、分析模型等进行分组管理，赋予使用者不同的权限；  4、★支持采集常见的虚拟环境日志，如Xen、VMWare、Hyper-V等。支持自动发现资产以提高配置效率。支持一键检测，可以直观地展示出系统主程序、定时任务、数据库监控等内容的检查结果及描述，同时给出处理意见，以便快速定位并处理故障问题。（需提供相关功能截图证明）  5、支持自定义解析规则，提供美观易用的思维导图模式。支持监控解析规则性能，支持展示规则名称、所属规则包、匹配成功或失败次数、成功或失败平均耗时等信息，同时可以一键启用或禁用解析规则。  6、★内置SOX、ISO27001、WEB安全等解决方案包以满足合规要求，同时支持根据需求上传解决方案包对产品进行功能扩展。用户登录支持双因子认证。支持日志转发、安全域同步至第三方平台等大数据联调功能。提供开放API接口，灵活对接第三方系统或二次开发日志应用。  7、支持基于内存的实时关联分析，跨设备的多台事件关联分析。支持导入自定义的关联规则文件。支持通过资产、安全知识库、弱点库三个维度的三维关联分析。支持导入资产弱点漏洞数据，兼容目前市场上主流的资产弱点扫描工具。产品内置CVE漏洞数据知识库、Web漏洞数据知识库等安全知识库。  8、支持性能监控，包括主机类、应用类。通过在目标主机上安装Agent程序监测目标主机的CPU使用率、内存使用率、磁盘使用率、磁盘使用情况、网络总流量等信息。  9、内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景，满足日常安全分析的大部分需求。  10、具有公安部信息安全产品检测中心出具的产品检验报告，检验报告须符合《信息安全技术日志分析产品安全技术要求 GA/T 911-2010》(第三级)，并提供完整的检测报告复印件（行标三级），设备原厂商具备为CMMI能力成熟度模型集成五级证书、CNCERT/CC网络安全应急服务支撑单位（国家级）、企业知识产权管理体系证书。 | 台 | 1 |
| 3 | 终端检测响应平台软件 | 1.产品包含管理控制中心及终端客户端软件，其中管理控制中心可云化部署也可以硬件一体部署；采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能，授权数量≥100个。  2.支持以安全策略模板方式对指定终端组快速部署安全策略，安全策略模板支持默认模板和自定义模板；  3. ★支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测和威胁处置方式、暴力破解的威胁处置方式和Windows白名单信任目录；  4.支持对主机账号信息进行梳理，可按照“7天”、“30天”展示登录历史，了解账号风险，包括是否存在隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、半夜登录、多IP登录等，并可以将存在风险账号的主机列表导出  5.支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等  6.支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz等自启动，可以防止黑客攻击  7. ★一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果（需提供相关功能截图证明）；  8.提供对业务系统之间、业务系统内不同应用角色之间、业务系统内相同应用角色之间的访问控制、微隔离策略配置；业务系统详情支持展示流量分布Top5、业务流量排行Top5(发送，接收)、业务访问趋势（发送流速、接收流速和用户数）  9.支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。  10.产品联动功能：支持将检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到安全态势感知平台，并在安全态势感知平台进行分析和展示；接收态势感知平台下发的快速查杀任务，并查看任务状态，结果并进行处置；一键隔离指令，对终端所有连接进行阻断，防止病毒进一步扩散支持接收下一代防火墙下发的快速查杀任务，并查看任务状态，结果并进行处置；一键隔离指令，对终端所有连接进行阻断，防止病毒进一步扩散；并对僵尸网络进行举证、溯源和联动查杀。  11. ★支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离。 | 套 | 1 |
| 4 | 防病毒网关模块 | 现有H3C S10510防火墙增配防病毒模块授权，3年原厂升级服务许可 | 套 | 1 |

# 投标人资格条件

1. 投标人须是具备完成本招标项目供货的独立法人，并免费提供技术咨询服务。
2. 资信良好，无不良记录。
3. 具有履行相关承诺的能力。投标单位须提供近3年3个类似已竣工项目的业绩证明材料(采购合同复印件并盖红章）。

# 验收要求

在合同签订后，由乙方制定《项目总体实施方案》，经甲方讨论并最终审核通过，作为本合同项目实施总纲领。在实施过程中，《项目总体实施方案》需要变更时，须双方协商达成一致，并双方盖章确认。

甲方应在设备运抵现场时，通知乙方安装计划，乙方必须于24小时内派遣工程师前往现场进行安装调试。**所有项目及设备的安装调试、集成配置须在合同签署后的30个工作日内施工完毕**。

系统调测完成后，乙方应书面通知甲方进行初验。整个合同系统符合本合同的技术规范要求和系统/设备验收标准，则双方应签署《系统/设备初验备忘录》。不合格产品不得进入试运行阶段。

初验合格后，进入试运行阶段。试运行期间，甲方进行合同项下设备的操作及维护，乙方给予技术协助。从《系统/设备初验备忘录》确定的试运行期起始日期起。**试运行期为三个月**。不合格产品不得进入终验阶段。

试运行结束后，整个合同系统符合本合同的技术规范要求和系统/设备验收标准，则双方依照合同规定签署《系统/设备终验备忘录》。

以“招投标文件参数”、“项目总体实施方案”及实验过程阶段产生的、经甲方项目领导小组成员确认签字的需求变更或分阶段内容调整内容为验收依据。

验收由甲方相关科室、甲方技术小组负责项目的整体验收工作，验收结果双方主管人员签字认可。

项目软件按照计算机软件工程规范国家标准分阶段提交相应文档系统交付包括但不限于如下交付内容实施计划、需求规格说明书、测试计划、测试报告、培训计划、试运行/上线报告、系统部署、软件用户使用手册、操作文档等。在项目整体验收阶段以电子版及打印件形式提交给甲方，甲方在接到全部文档后应该签署文档清单。

合同项目的验收并不能免除乙方对合同设备项目的保证责任。在设备系统安装调试、初验测试、试运行和终验测试时发现设备（系统）不符合合同约定的技术规范要求和验收标准而乙方未在约定期限内及时采取措施予以补救的，甲方有权要求退货，收回全部已付款，并要求乙方赔偿因此而造成的所有损失。

# 其它要求

本项目为交钥匙工程，所有设备满配光纤模块（包括对端交换机模块）、以及项目中所涉及到的所有辅材（如网线、光纤等）。投标报价须包括项目内所有设备的费用、包装、运输、安装、调试、集成、试运行、对接运行、人员培训、技术资料、保险、配件、质保期内费用(含系统部署及迁移期间的人员保证及相关费用)、各种税费等项内容的全部费用，并考虑相关风险。

本项目涉及的所有工程、设备及软件系统需满足等级保护二级要求。承建单位负责协助学校完成本项目中所涉及的等级保护测评相关工作。

所有设备及系统须提供三年原厂维保服务。包括硬件质保、软件升级、病毒库、URL升级。维保过后需免费提供技术咨询服务。原厂服务需提供相关证明。

设备质保期过后可根据需要进行病毒库和规则库的升级，终端检测响应平台软件病毒库和规则库升级按照不高于合同单价的25%/年价格，中间断保不再收费。

各项目涉及的厂商需提供本地化服务，在出现问题故障后保证1小时到达现场，2小时解决问题。